CLAIMS

We claim:

1. A Video-on-Demand method for demanding a video program via a short message, comprising the steps of:

generating, at a user end, a demand short message including information on the demanded video program, said demand short message including at least a User Identifier field, a Program Identifier field of the demanded video program and an Authentication field;

sending to a program delivering end the generated demand short message;

receiving the demand short message at the program delivering end, and processing the received demand short message to extract a user identifier and using the Authentication field to authenticate legality of the user;

after authenticating the legality of the user successfully, sending program content corresponding to a program identifier from the program delivering end to the user end indicated by the user identifier; and

receiving the demanded video program at the user end.

2. A Video-on-Demand method according to claim 1, further comprising the step of sending from the program delivering end to the user end a reply message including a confirmation message indicating that the demand short message has been received.

3. A Video-on-Demand method according to claim 1, further comprising the steps of:

encrypting the fields in the generated demand short message except the Authentication field at the user end, and

decrypting the received encrypted short message at the program delivering end to extract the user identifier and the program identifier.

4. A Video-on-Demand method according to claim 1, wherein said demand short message further comprising:

a Format Identifier field for defining a format of said demand short message;

a Demand Time field for indicating a time for sending said demand;

a Playback Time field for indicating a start time of video playing;

an Optional field containing optional data that may describe said demand more precisely; and

said Authentication field is an encrypted digest of the above User Identifier field, Program Identifier field, Format Identifier field, Demand Time field, Playback Time field, and Optional field.

5. A Video-on-Demand method according to claim 4, wherein said Authentication field is generated according to the following procedure:

calculating the digest of all the fields except the Authentication field using a digest algorithm;

encrypting with a cipher algorithm a calculated digest by adopting a secret authentication key corresponding to a user end device, uniquely allocated in advance by the program delivering end; and

a process of authenticating a user's legality by the program delivering end being conducted according to the following procedures:

calculating the digest of all the fields except the Authentication field using a digest algorithm;

encrypting with a cipher algorithm the calculated digest by adopting a secret authentication key corresponding to a user end device, uniquely allocated in advance by the program delivering end, so as to calculate an Authentication field; and

checking whether the calculated Authentication field and the received Authentication field are identical.

6. A Video-on-Demand method according to claim 5, wherein when said video program is sent via a conditional access system, a content key is delivered with the video program, so there is no need for a separate deliver of said reply message.

7. A Video-on-Demand method according to claim 5, wherein when the video program demanded by the user needs to be encrypted and the encrypt key is not sent via a conditional access system, the method further comprising the steps of:

generating, at the program delivering end, an encrypted reply message containing a content key of said video program, and sending it to the user end;

decrypting, at the user end, the content key from said encrypted reply message; and

decrypting the video program received from the program delivering end according to the decrypted content key.

8. A Video-on-Demand method according to claim 7, wherein said encrypted content key is encrypted using a device key corresponding to the user end device, uniquely allocated in advance by the program delivering end, and said device key can be different from said Authentication key.

9. A Video-on-Demand system for demanding a video program via a short message, comprising:

short message generating means for receiving a user demand, and generating a demand short message based on the user demand, said demand short message including at least a User Identifier field, a Program Identifier field of the demanded video program and an Authentication field;

short message sending means for sending the demand short message generated by the short message generating means;

demand short message processing means at a program delivering end for receiving the demand short message, processing the received demand short message to extract the user identifier and using the Authentication field to authenticate the legality of the user,

and sending the program identifier of the demanded program by a legal user to video delivering means;

video delivering means for sending program content corresponding to the program identifier from the program delivering end to the user end indicated by a legal user identifier; and

program playing means at the user end for receiving the video program sent by the video delivering means and playing it back to the user.

10. A Video-on-Demand system according to claim 9, wherein the demand short message processing means further comprises a reply message generating unit for generating a reply message including at least a confirmation message indicating that the demand short message has been received, for sending to the user end.

11. A Video-on-Demand system according to claim 9, wherein:

the short message generating means further comprises an encrypting unit for encrypting the fields in the generated demand short message except the Authentication field; and

the demand short message processing means further comprises decrypting means for decrypting the received encrypted short message.

12. A Video-on-Demand system according to claim 9, wherein said short message generating means further comprises a program information generating unit for generating said User Identifier field, said Program Identifier field of the video program demanded by the user and

a Format Identifier field for defining a format of said demand short message,

a Demand Time field for indicating a time for sending said demand,

a Playback Time field for indicating a start time of video playing, and

an Optional field containing optional data that may describe said demand more precisely.

13. A Video-on-Demand system according to claim 12, wherein

said short message generating means further comprises an Authentication field generating unit for calculating a digest of all the fields except the Authentication field using a digest algorithm and encrypting with a cipher algorithm the calculated digest by adopting a secret authentication key corresponding to a user end device, uniquely allocated in advance by the video delivering means; and

said demand short message processing means further comprises an authentication unit for calculating the digest of said User Identifier field, Program Identifier field, Format Identifier field, Demand Time field, Playback Time field and Optional field, encrypting with a cipher algorithm the calculated digest by adopting a secret authentication key corresponding to a user end device, uniquely allocated in advance by the video delivering means, so as to calculate an Authentication field and checking whether the calculated Authentication field and the received Authentication field are identical.

14. A Video-on-Demand system according to claim 13, wherein if said video program is sent via a conditional access system, a content key is delivered with the video program.

15. A Video-on-Demand system according to claim 13, wherein if the video program demanded by the user needs to be encrypted and the encrypt key is not sent via a conditional access system, then

the demand short message processing means generates an encrypted reply message containing a content key of said video program, and sends it to the user end; and

the program playing means at the user end decrypts the content key from said encrypted reply message, and decrypts the video program received from the program playing means according to the decrypted content key.

16. A Video-on-Demand system according to claim 15, wherein said encrypted content key is encrypted using a device key corresponding to the user end device, uniquely allocated in advance by the program delivering end, and said device key can be different from said Authentication key.

17. Short message generating means in a Video-on-Demand system, comprising:

a receiving unit for receiving a user demand;

a program information generating unit for generating, according to the user demand, program information including at least a User Identifier field and a Program Identifier field of the demanded video program;

an Authentication field generating unit for generating a Authentication field according to the program information generated by the program information generating unit; and

an output unit for outputting said program information and the Authentication field as a demand short message to short message sending means.

18. A short message generating means according to claim 17, further comprising:

an encrypting unit for encrypting the fields except the Authentication field in the demand short message.

19. A short message generating means according to claim 17, wherein said program information generating unit further generating:

a Format Identifier field for defining a format of said demand short message,

a Demand Time field for indicating the time for sending said demand,

a Playback Time field for indicating the start time of video playing, and

an Optional field containing optional data that may describe said demand more precisely.

20. A short message generating means according to claim 19, wherein

said Authentication field generating unit calculates the digest of all the fields except the Authentication field using a digest algorithm and encrypts with a cipher algorithm the calculated digest by adopting a secret authentication key determined in advance and uniquely corresponding to said short message generating apparatus.

21. A short message generating means according to claim 20, wherein said digest algorithm is MD5 algorithm, and said cipher algorithm is 3DES algorithm.

22. A short message generating method in a Video-on-Demand system, comprising the steps of:

receiving a user demand;

generating, according to the user demand, program information including at least a User Identifier field and a Program Identifier field of a demanded video program;

generating an Authentication field according to the generated program information; and

outputting said program information and the Authentication field as a demand short message to short message sending means.

23.. Demand short message processing means in a Video-on-Demand system, comprising:

a receiving unit for receiving a demand short message;

an extracting unit for extracting a user identifier from the demand short message received by the receiving unit;

an authentication unit for authenticating legality of a user identified by the user identifier extracted by the extracting unit, according to the Authentication field in the demand short message received by the receiving unit; and

an outputting unit for outputting a program identifier of the program which the legal user demands.

24. A demand short message processing method in a Video-on-Demand system, comprising the steps of:

receiving a demand short message;

extracting a user identifier from the received demand short message;

authenticating legality of a user identified by the extracted user identifier, according to the Authentication field in the received demand short message; and

outputting a program identifier of the program which the legal user demands.

25. An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing Video-on-Demand, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 1.

26. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for Video-on-Demand, said method steps comprising the steps of claim 1.

27. A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing Video-on-Demand, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of claim 9.

28. A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing short message generation, the computer readable program code means in said computer program product

comprising computer readable program code means for causing a computer to effect the functions of claim 17.

29. An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing short message generation, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 22.

30. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for short message generation, said method steps comprising the steps of claim 22.

31. A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing short message generation, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of claim 23.

32. An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing demand short message processing, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 24.

33. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for demand short message processing, said method steps comprising the steps of claim 24.